Curves with sharp Chabauty-Coleman bound

Gajovic, Stevan

Published in:
ArXiv

Publication date:
2020

Curves with sharp Chabauty-Coleman bound

Stevan Gajović

Abstract

We construct curves of each genus $g \geq 2$ for which Coleman's effective Chabauty bound is sharp and Coleman's theorem can be applied to determine rational points if the rank condition is satisfied. We give numerous examples of genus two and rank one curves for which Coleman's bound is sharp. Based on one of those curves, we construct an example of a curve of genus five whose rational points are determined using the descent method together with Coleman's theorem.

Contents

1 Introduction

One of the fundamental problems in the arithmetic of curves and abelian varieties is to find ways to use p-adic information on curves to determine rational points. It is

known that p-adic points have a richer structure than rational points, and, in principle, are easier to determine. Thus, it is natural to try to use the knowledge of p-adic points in studying rational points. There are several such approaches, e.g., the Hasse principle and its generalizations, or bounding ranks of elliptic curves by Selmer groups.

The method of Chabauty and Coleman, nowadays also called "abelian Chabauty," is a powerful p-adic method, and very successful in determining rational points on curves satisfying a certain rank condition. Coleman's "effective Chabauty" theorem (theorem 2) gives an upper bound on the number of rational points on these curves. However, it is rare that the direct application of Coleman's theorem succeeds in determining all rational points because the bound from Coleman's theorem is not sharp in most cases.

In fact, there are only a few curves known for which Coleman's bound is sharp. Hence it is of interest to study the question highlighted by Coleman's result: Regardless of the rank of its Jacobian, when does the number of rational points on C meet or exceed Coleman's bound at p? We will call curves for which the rank condition is satisfied, and Coleman's bound is sharp for some prime number p of good reduction, *sharp curves at* p. The curves such that the number of their known rational points meets Coleman's bound regardless of the rank condition will be called *potentially sharp curves at* p. Note that we cannot use the method of Chabauty and Coleman to determine the set $C(\mathbb{Q})$ for potentially sharp curves C because we did not check the rank condition. However, if the rank condition holds for a potentially sharp curve, then the curve is sharp; hence, we determined its rational points. Curves that exceed the bound will be called *excessive at* p. Curves for which there is a prime p such that the curve is sharp at p, potentially sharp at p, or excessive at p are called sharp, potentially sharp, and excessive, respectively. We note that the rank of the Jacobians of excessive curves is at least g.

We concisely introduce the method in § 1.1, and the computations of the rank of Jacobians of hyperelliptic curves in § 1.2. In § 1.3, we briefly present the descent method for determining rational points on curves. The descent method is usually used to descend to curves of genus zero and one. Thus, in § 2.3, we construct a curve whose rational points are determined by using descent to curves of genus two, and one of them is sharp.

After mentioning two known sharp curves in § 2.1, we give various examples of sharp curves of genus two in § 2.2, and one with the smallest number of rational points in § 2.4. In § 2.5 we list two curves which violate Coleman's bound, and we use this information to determine their ranks.

In the third chapter, we start by presenting sharp curves of genus three, four, and

five in § 3.1. Using results on the existence of primes in short intervals, we construct infinitely many potentially sharp curves of each genus $g \geq 2$ in § 3.3. We give examples of sharp curves of genus $g = 4$ and $g = 5$ based on this construction.

All computations were done in Magma, [BCP97].

1.1 The method of Chabauty and Coleman and its history

In 1922, in [Mor22], Louis J. Mordell proved that the group of rational points of an elliptic curve $E/\mathbb{Q}$ is finitely generated. At the end of the article, Mordell observes that curves of genus $g \geq 2$ have only finitely many rational points. The statement that for a nice (smooth, projective, and geometrically irreducible) curve C of genus $g \geq 2$ and a number field K it holds that $\#C(K)$ is finite was named the "Mordell conjecture". After Mordell's theorem it was a natural question whether the group $A(K)$ is finitely generated for all abelian varieties A/K, where K is any number field. In 1928, André Weil proved in [Wei29] that for all abelian varieties A over the number field K we have

$$A(K) \cong \mathbb{Z}^r \oplus A(K)_{\text{tors}},$$

where $A(K)_{\text{tors}}$ is the torsion subgroup of $A(K)$ and $r \in \mathbb{N}_0$ is called the rank of $A(K)$.

In the 1940s, Claude Chabauty proved the Mordell conjecture for curves that satisfy a certain condition.

Theorem 1. *(Chabauty 1941, [Cha41]) Let C be a nice curve of genus $g \geq 2$. Let $J(C)$ be its Jacobian, and let r be the rank of $J(C)$ over $\mathbb{Q}$. If $r < g$, then $C(\mathbb{Q})$ is finite.*

We briefly discuss the idea behind the proof. We may assume that $C(\mathbb{Q}) \neq \emptyset$ and embed $C(\mathbb{Q})$ via an Abel-Jacobi map into $J(C)(\mathbb{Q})$, and do the same over the field $\mathbb{Q}_p$, where p is a prime of good reduction for C. That means that $\overline{C}$, the curve which is obtained by reduction of C modulo p, remains a smooth curve over $\mathbb{F}_p$. We have the following commutative diagram.

$$\begin{array}{ccc} C(\mathbb{Q}) & \hookrightarrow & J(C)(\mathbb{Q}) \\ \downarrow & & \downarrow \\ C(\mathbb{Q}_p) & \hookrightarrow & J(C)(\mathbb{Q}_p) \end{array}$$

The set $J(C)(\mathbb{Q}_p)$ has the structure of a g-dimensional p-adic manifold, containing $C(\mathbb{Q}_p)$ as a 1-dimensional submanifold. The discrete group $J(C)(\mathbb{Q})$ also sits inside $J(C)(\mathbb{Q}_p)$, and we take its closure in the p-adic topology of $J(C)(\mathbb{Q}_p)$, denoted by $\overline{J(C)(\mathbb{Q})}$, to make it a submanifold of $J(C)(\mathbb{Q}_p)$. Then the dimension of $\overline{J(C)(\mathbb{Q})}$ is not greater than r, so heuristically for dimensional reasons, it should have finite intersection with $C(\mathbb{Q}_p)$, which was what Chabauty proved. This intersection contains the set $C(\mathbb{Q})$ (more precisely, $C(\mathbb{Q})$ injects into it), implying the finiteness of $C(\mathbb{Q})$.

This theorem remained the most significant result towards the Mordell conjecture until Gerd Faltings proved the conjecture unconditionally, i.e. for all nice curves of genus $g \geq 2$, in [Fal83]. It seemed that Chabauty's theorem lost its value. But, that is not true because Robert Coleman in 1985 found a way to use Chabauty's approach to state and prove an effective version of the theorem.

Theorem 2. *(Coleman 1985, [Col85a]) Let C be a nice curve of genus $g \geq 2$. Let $J(C)$ be its Jacobian, and let r be the rank of $J(C)(\mathbb{Q})$. Let p be a prime of good reduction for C. If $r < g$, and $p > 2g$, then*

$$\#C(\mathbb{Q}) \leq \#\overline{C}(\mathbb{F}_p) + 2g - 2.$$

Coleman invented a theory of p-adic integration on curves in [Col85b], which has properties that we would expect from integration, such as linearity in integrands and additivity in endpoints. When two endpoints are in the same residue disc, i.e., when both have the same reduction modulo p, we can compute the integral in the expected way by expressing the integrand as a power series in a local parameter and then integrating term by term. There are more important properties, such as Frobenius equivariance, and unexpectedly, path-independence, unlike the real and complex case. The last two properties turn out to be very convenient, and all properties together make Coleman integrals practically computable, which makes Chabauty's method effective. Using Coleman integration, we can construct a locally analytic function $\rho : C(\mathbb{Q}_p) \longrightarrow \mathbb{Q}_p$, which vanishes on $C(\mathbb{Q})$. We can estimate the number of zeros in each residue disc, and summing all estimates gives us the bound in theorem 2.

We can furthermore investigate the function ρ in each residue disc (and sometimes combine results with some other methods) to provably determine $C(\mathbb{Q})$. This locally analytic function ρ is the main ingredient in determining rational points on curves, and it is a main object of research nowadays to extend the method to the complimentary case $r \geq g$. This is an explicit version of a non-abelian extension of this method, a program initiated by Kim in [Kim05] when $r \geq g$. The special case when $r = g$ is called Quadratic Chabauty, because then, instead of linear functionals (integrals), we use quadratic functions (p-adic heights) to determine rational points. The first explicit examples can be found in [BBM16].

By a careful investigation inside each residue disc, Michael Stoll in [Sto06] proved a theorem that improves Coleman's bound.

Theorem 3. *(Stoll 2006, [Sto06]) Let C be a nice curve of genus $g \geq 2$. Let $J(C)$ be its Jacobian, and let r be the rank of $J(C)$ over $\mathbb{Q}$. Let p be a prime of good reduction for C. If $r < g - 1$, and $p > 2r + 2$, then*

$$\#C(\mathbb{Q}) \leq \#\overline{C}(\mathbb{F}_p) + 2r.$$

As a corollary, we have the following rank statement for sharp curves. We know that $r < g$. If $r < g - 1$, then Coleman's bound cannot be sharp.

Corollary 4. *Let C be a sharp curve of genus $g \geq 2$. Then the rank of the Jacobian of C over $\mathbb{Q}$ is $r = g - 1$.*

If a curve satisfying the rank condition is not sharp, this means that looking at the local information at p is not sufficient to determine its rational points. Nevertheless, it is often possible to compute the rational points by combining the Chabauty information at p with v-adic information for other primes v, for instance, obtained through the Mordell-Weil sieve. The Mordell-Weil sieve was introduced in [Sch99], and well explored in the paper [BS10]. We also note that the Mordell-Weil sieve can be successfully combined with the Quadratic Chabauty method, see, e.g., [BBM17].

One reference for more details about the method of Chabauty and Coleman is [MP12]. The notes [Sik15] contain some very explicit examples, including the combination of the method the Mordell-Weil sieve.

1.2 On the computation of the rank of the Jacobian of hyperelliptic curves

The problem of computing the rank of abelian varieties is extremely difficult in general and still open. It is related to one of the most important conjectures in arithmetic geometry. This is the Birch and Swinnerton-Dyer conjecture, which states that the rank of an abelian variety can be computed analytically, namely, as the order of vanishing of its L-function at $s = 1$ (for more details see, e.g., [Tat66]). The latter quantity is called the analytic rank. Thus, if one is willing to assume the Birch and Swinnerton-Dyer conjecture, then the rank of hyperelliptic curves can be computed as an analytic rank. We can compute the L-function of hyperelliptic curves in Magma using the algorithm by Dokchitser, [Dok04], and we can evaluate it at $s = 1$ as well as its derivatives. We need to be careful that we can compute these values only up to some precision. In general, we cannot prove that some value is zero, although we can verify that it is very close to zero.

Algebraically, there has been a lot of progress since Weil's theorem, and there are methods that work in many cases, but none of them is guaranteed to work, even for the simplest case of elliptic curves. One of the first explicit computations for dimension greater than one appeared in the paper [GG93], followed by [Sch95]. It was later generalized and implemented for hyperelliptic curves in Magma by Stoll, [Sto01].

Let J be the Jacobian of hyperelliptic curve $C : y^2 = f(x)$. From the Kummer exact sequence $0 \longrightarrow J[2] \longrightarrow J \xrightarrow{[2]} J \longrightarrow 0$, and the long exact sequence of Galois cohomology we get the commutative diagram ($M_{\mathbb{Q}}$ is the set of places of $\mathbb{Q}$)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J(\mathbb{Q})/2J(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, J[2]) & \longrightarrow & H^1(\mathbb{Q}, J)[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & \overset{\alpha}{\searrow} & \downarrow & & \\ 0 & \longrightarrow & \prod_{v \in M_{\mathbb{Q}}} J(\mathbb{Q}_v)/2J(\mathbb{Q}_v) & \longrightarrow & \prod_{v \in M_{\mathbb{Q}}} H^1(\mathbb{Q}_v, J[2]) & \longrightarrow & \prod_{v \in M_{\mathbb{Q}}} H^1(\mathbb{Q}_v, J)[2] & \longrightarrow & 0 \end{array}$$

The kernel of the map α is *the Selmer group* $\mathrm{Sel}^{(2)}(J/\mathbb{Q})$, and the kernel

$$Ш(\mathbb{Q}, J) := \ker\left(H^1(\mathbb{Q}, J) \longrightarrow \prod_{v \in M_{\mathbb{Q}}} H^1(\mathbb{Q}_v, J)\right)$$

is called *the Shafarevich-Tate group*.

We have the following exact sequence from the diagram above

$$0 \longrightarrow J(\mathbb{Q})/2J(\mathbb{Q}) \longrightarrow \mathrm{Sel}^{(2)}(J/\mathbb{Q}) \longrightarrow Ш(\mathbb{Q}, J)[2] \longrightarrow 0.$$

It is a well-known fact that $\mathrm{Sel}^{(2)}(J/\mathbb{Q})$ is a finite group. The idea of the proof, which works for more general Selmer groups, and can be found in, e.g., [HS00, C.4], is to construct an injection into a finite commutative group indexed by bad and infinite primes. In [HS00, C.4], we also see that the Selmer group is, in principle, effectively computable. We have

$$\dim_{\mathbb{F}_2} J(\mathbb{Q})/2J(\mathbb{Q}) = r + \dim_{\mathbb{F}_2} J(\mathbb{Q})[2] \leq \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}(J/\mathbb{Q}).$$

The difference between two sides is exactly $\dim_{\mathbb{F}_2} Ш(\mathbb{Q}, J)[2]$.

We can easily determine $J(\mathbb{Q})[2]$, it depends on the factorization of f over $\mathbb{Q}$. Thus, we can obtain an upper bound on the rank of $J(\mathbb{Q})$.

For the lower bound, we search for rational points on J, up to some bounded height, and hope that eventually, we will find the same number of independent points as the upper bound for the rank. If the curve has many rational points, then we might be able to find a lower bound on the rank, see the remark in 2.5.

From the algorithm, we easily see why it is not guaranteed to work, but it still works very well in practice. We also see that the (partial) knowledge of $Ш(\mathbb{Q}, J)$ can improve upper bounds, e.g., as in [Sto01, Chapter 8].

1.3 Introduction to the descent method

The descent method is one of the first methods ever used for determining rational points on curves. It is still very applicable, especially for hyperelliptic curves. The basics of this method are explained in more detail in [Sto15]. For explicit descent on hyperelliptic curves, see [BS09]. The descent method is based on the property of unique factorization in $\mathbb{Z}$. In a sense, it is a generalization of the fact that if a product of two numbers is a square, then these two numbers have the same squarefree

part. We can bound the possible greatest common divisor of these numbers which gives only finitely many possibilities for their squarefree parts. In principle, we have a strategy to reduce all possible factorizations to a finite number.

Let us make it more precise. Suppose that $C/\mathbb{Q}$ is a hyperelliptic curve given by the equation

$$C : y^2 = f_1(x)f_2(x),$$

where f_1 and f_2 are non-constant coprime integral polynomials, with at least one of $\deg(f_1)$ and $\deg(f_2)$ even. Then, for every point $(x_0, y_0) \in C(\mathbb{Q})$, we have $f_1(x_0) \neq 0$ or $f_2(x_0) \neq 0$, and there is a unique squarefree $d \in \mathbb{Z}$, and $z_0, t_0 \in \mathbb{Q}$, such that

$$f_1(x_0) = dz_0^2, \quad f_2(x_0) = dt_0^2.$$

Denote by C_d the curve given by equations

$$C_d : f_1(x) = dz^2, \quad f_2(x) = dt^2,$$

then there is a covering $\pi_d : C_d \longrightarrow C$ given by

$$(x, z, t) \mapsto (x, dzt).$$

It follows that

$$C(\mathbb{Q}) = \bigcup_{d \in S} \pi_d(C_d),$$

where $S \subset \mathbb{Z}$ denotes the set of all squarefree numbers. This set is infinite, but we can reduce it to a finite set. Let us assume that f_1 and f_2 are monic polynomials (otherwise, we have to include primes that divide their leading coefficients). As these polynomials are coprime, their resultant is a non-zero integer R. The resultant gives information on possible common roots. So, for all primes p such that $p \nmid R$, the resultant of f_1 and f_2 over $\mathbb{F}_p$ is not zero, implying that f_1 and f_2 do not have a common root in $\mathbb{F}_p$. It means that f_1 and f_2 are "coprime at p", i.e., that it is not possible that p divides the squarefree part d. So, the number of possible primes which can divide the squarefree part d is finite, and we need to investigate a finite number of curves C_d (which, in principle, should be easier than doing so for C) to find all rational points on C.

1.4 Acknowledgements

The author is funded by the DFG-Grant MU 4110/1-1. Part of this research was done during the "Summer school in computational number theory" in Bristol and during a visit to Boston University where the author was partially supported by the Diamant PhD Travel Grant. The author thanks Steffen Müller for his support, checking examples and numerous comments and corrections on the text, Jennifer Balakrishnan, Francesca Bianchi, Céline Maistret, Michael Stoll, and Jaap Top for

useful discussions, Pieter Moree for significant help on obtaining the special case of Bertrand's postulate used here, Lazar Radičević for many suggestions and checking examples, Alex Best for helpful suggestions, Oana Adascalitei for help and support when creating examples, and Boston University for their hospitality and providing Magma on their computer. The author thanks the anonymous referees for carefully reading the article and many useful comments.

2 Examples of sharp curves of genus two

2.1 Two known sharp curves in genus two

We first mention two known examples.

Example 1.([Gra94]) This is the first known example of a sharp curve, so we see that it took almost ten years after Coleman's paper [Col85a] until the first example appeared. Let C be the curve given by the equation

$$C : y^2 = x(x-1)(x-2)(x-5)(x-6).$$

This curve has good reduction at $p = 7$, and it has eight $\mathbb{F}_7$-rational points

$$\overline{C}(\mathbb{F}_7) = \{(0,0), (1,0), (2,0), (3,\pm 1), (5,0), (6,0), \infty\}.$$

In [GG93], it is computed that $J(C)(\mathbb{Q}) \cong \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^4$. We can apply theorem 2 to obtain that $C(\mathbb{Q}) \leq 8 + 2 = 10$. We can find ten rational points, so

$$C(\mathbb{Q}) = \{(0,0), (1,0), (2,0), (3,\pm 6), (5,0), (6,0), (10,\pm 120), \infty\}.$$

Example 2.([HM19]) This example is miraculous because it arises from a geometric problem. Namely, this curve occurs in analysing the problem whether there exists a pair of one right triangle and one isosceles triangle, both with rational sides, having the same area and perimeter. More details about the problem can be found in [HM19]. The curve C is given by the equation

$$C : y^2 = (x^3 - x + 6)^2 - 32.$$

We compute that the rank of its Jacobian over $\mathbb{Q}$ is equal to $r = 1$, that C has good reduction at $p = 5$, and that its reduction modulo 5 has exactly eight points. All conditions for theorem 2 are satisfied, thus we conclude

$$C(\mathbb{Q}) = \left\{(0,\pm 2), (1,\pm 2), (-1,\pm 2), \left(\frac{5}{6}, \pm\frac{217}{216}\right), \infty_{\pm}\right\}.$$

2.2 A finite family of sharp curves of genus two

We construct new examples of sharp curves of genus two. Let C be a curve. We focus on genus two curves because the computation of the rank becomes more difficult for larger genus. Thus, the bound is given by

$$\#C(\mathbb{Q}) \leq \#\overline{C}(\mathbb{F}_p) + 2.$$

Since we want this bound to be sharp, we would like that two residue discs have extra points (this condition is natural due to the hyperelliptic involution), and other ones to have exactly one rational point. The easiest way to achieve it is to require a small number of residue discs. We will construct a suitable monic polynomial $f(x)$ of degree 5. One natural choice for a prime p to consider is $p = 11$, because $x^5 \equiv 0, \pm 1 \pmod{11}$. If we want to include other monomials in x, we want them to have a coefficient divisible by 11, to control the polynomial $f(x)$ modulo 11 easily. It remains to pick the constant term. We want some constant for which we can find rational points, but not too many modulo 11. Quadratic residues modulo 11 are in the set $\{0, 1, 3, 4, 5, 9\}$, so if we pick the constant term to be 9 modulo 11, we have that

$$f(x) \equiv x^5 + 9 \equiv \{8, 9, 10\} \pmod{11}.$$

This implies that

$$\overline{C}(\mathbb{F}_{11}) = \{(0, \pm 3), \infty\}.$$

When the rank of the Jacobian of C over $\mathbb{Q}$ is less than two, by Coleman's bound, C can have at most 5 rational points.

Note, as in [Gra94], that we should check if a curve C has absolutely irreducible Jacobian. If this were not the case, then $J(C)$ would be isomorphic to the product of two elliptic curves over some number field K, and one of them would have rank zero, providing an easier way to determine rational points on C. In [Gra94], David Grant together with Jaap Top, proved absolute simplicity of the Jacobian of the curve from example 1 by proving that its L-function cannot be a product of two L-functions of elliptic curves. In the meantime, in [HZ02], Everett W. Howe and Hui J. Zhu found a criterion when an abelian variety over a finite field is absolutely simple.

Lemma 5. *([HZ02, Lemma 8]) Let q be a prime power and $n > 2$ an integer. Suppose that π is an ordinary Weil q-number (the minimal polynomial for π is a characteristic polynomial of Frobenius of an ordinary abelian variety). Let $K = \mathbb{Q}(\pi)$, K^+ its maximal real subfield, and $n = [K^+ : \mathbb{Q}]$. Suppose that*
(1) the minimal polynomial of π is not of the form $x^{2n} + ax^n + q^n$,
(2) the field K^+ has no proper subfields other than $\mathbb{Q}$,
(3) the field K^+ is not the maximal real subfield of a cyclotomic field.
Then the isogeny class corresponding to π consists of absolutely simple abelian varieties.

We finally give a number of examples.

Proposition 6. *Let $C_k : y^2 = f(x)$ be a hyperelliptic curve over $\mathbb{Q}$, where*

$$f(x) = x^5+11x^4+(11k+3)^2, \;\; k \in \{0,1,2,3,7,10,11,12,15,21,22,31,40,42,44,47,50\}$$

or

$$f(x) = x^5 + 11x^4 + (11k-3)^2, \;\; k \in \{1,4,9,15,16,17,19,27,28,31,40,41,42,43\}.$$

(1) Then $\#C_k(\mathbb{Q}) = 5$, and in the first case

$$C_k(\mathbb{Q}) = \{(0, \pm(11k+3)), (-11, \pm(11k+3)), \infty\},$$

whereas in the second case

$$C_k(\mathbb{Q}) = \{(0, \pm(11k-3)), (-11, \pm(11k-3)), \infty\}.$$

(2) All curves C_k from (1) have absolutely simple Jacobian.

Proof. (1) In both cases, we run the Magma command `RankBound` to compute an upper bound on the rank of the Jacobian of curves C_k for $0 \leq k \leq 50$. We listed above all k's in both cases for which the upper bound is less than two. As we saw, $p = 11$ is a prime of good reduction of all curves C_k and $\#\overline{C_k}(\mathbb{F}_{11}) = 3$, so we conclude by theorem 2 that $\#C_k(\mathbb{Q}) \leq 5$. The fact that we have five obvious rational points on each C_k finishes the proof. All listed curves C_k are sharp and have rank $r = 1$.

(2) Using Magma and lemma 5 we check that all $J(C_k)$ are absolutely simple by finding a prime p such that the reduction of $J(C_k)$ modulo p is absolutely simple. □

2.3 An example with descent and a sharp curve

There are many examples of applying descent from curves of higher genus to curves of genus zero or one in the literature. Lack of examples of curves whose rational points can be determined by applying descent to curves of genus at least two motivated us to construct one such curve.

Proposition 7. *Let $C/\mathbb{Q}$ be the hyperelliptic curve given by the equation*

$$C : y^2 = f(x) := (x^6 + 11x^5 + 64x + 729)(x^5 + 11x^4 + 64).$$

The set of rational points on C is

$$C(\mathbb{Q}) = \{(0, \pm 216), (-11, \pm 40), \infty\}.$$

Proof. As we can see, the polynomial f is monic, so when applying the descent method we need to compute the resultant of two polynomials, whose product is f, which is

$$R := \mathrm{Res}(x^6 + 11x^5 + 64x + 729, x^5 + 11x^4 + 64)) = 3^{30}.$$

We are only interested in the radical of the resultant, since it is enough to consider squarefree numbers, and $\mathrm{rad}(R) = 3$. Thus, after applying the descent, we know that x corresponds to an x-coordinate of a rational point on one of curves

$$x^5 + 11x^4 + 64 = dz^2, \quad x^6 + 11x^5 + 64x + 729 = dt^2$$

for some $d \in \{-3, -1, 1, 3\}$.

We first prove that $d < 0$ is impossible. If $x^5 + 11x^4 + 64 < 0$, then $x < 0$ and so

$$x(x^5 + 11x^4 + 64) + 729 > 0,$$

giving a contradiction.

If $d = 3$, then we can use the linear change of coordinates $X = 3x$, $Y = 3^3 z$, and then the equation of the curve

$$C_3 : x^5 + 11x^4 + 64 = 3z^2$$

transforms to

$$C_3' : X^5 + 33X^4 + 64 \cdot 3^5 = Y^2.$$

For the curve C_3', we compute in Magma that $J(C_3')(\mathbb{Q}) = \langle 0 \rangle$. We know that $C_3'(\mathbb{Q})$ embeds into $J(C_3')(\mathbb{Q})$, so C_3' has at most one rational point, this is the one at infinity.

If $d = 1$, then we consider the hyperelliptic curve

$$C_1 : x^5 + 11x^4 + 64 = z^2,$$

which is one of curves in proposition 6, and we already know

$$C_1(\mathbb{Q}) = \{(0, \pm 8), (-11, \pm 8), \infty\}.$$

We see that all of these points give rise to the rational points of C, and that

$$C(\mathbb{Q}) = \{(0, \pm 216), (-11, \pm 40), \infty\}.$$

□

Comment. Under assuming the Generalized Riemann Hypothesis, Magma gives that, $2 \leq r \leq 4$, where r is the rank of the Jacobian of C over $\mathbb{Q}$. So, in principle, we would be able to apply abelian Chabauty method to C. However, this seems to be more difficult than the approach in the proof, which is furthermore unconditional. As we can check in Magma, the Jacobian of C is absolutely simple.

2.4 A sharp curve with the smallest possible number of points

We give an example of a sharp curve that satisfies the property that it has the smallest number of rational points amongst all sharp curves of genus $g \geq 2$. For a sharp curve C of genus $g \geq 2$ it holds $\#C(\mathbb{Q}) \geq 3$. Indeed, we know that in that case

$$\#C(\mathbb{Q}) = \#\overline{C}(\mathbb{F}_p) + 2g - 2 \geq \#\overline{C}(\mathbb{F}_p) + 2 \geq 2.$$

Therefore, the set $C(\mathbb{Q})$ is non-empty, implying that also $\overline{C}(\mathbb{F}_p)$ is non-empty, giving the desired conclusion. If we want to construct such a curve, we want a curve of genus two, with only one residue disc. If we consider a hyperelliptic curve $C : y^2 = f(x)$, where f is a monic polynomial of degree 5, we already know that we have one residue disc, at infinity. So, we want to construct a curve having no other residue discs, meaning that the reduction over $\mathbb{F}_p$ can have only the point at infinity. We will use a similar strategy as before, so that

$$\overline{C} : y^2 = x^5 + c/\mathbb{F}_{11}.$$

If $c \equiv 7 \pmod{11}$, then $\overline{C}$ has only one rational point, $\overline{C}(\mathbb{F}_{11}) = \{\infty\}$ because 6, 7, and 8 are not quadratic residues modulo 11, and C has good reduction at $p = 11$. There should be two more rational points on C. Let one of them be $P = (a, b)$. Then P maps to infinity modulo 11. Furthermore, we know that the denominator of a is divisible by 11^2 since otherwise $f(a)$ is not a square of a rational number. Let us try to find an example such that a is already a square of a rational number and that a is a zero of a polynomial $f(x) - x^5$, with f satisfying the conditions above.

Let C be the hyperelliptic curve over $\mathbb{Q}$ defined by

$$C : y^2 = x^5 + 121x - 4.$$

Magma gives us that r, the rank of the Jacobian of C over $\mathbb{Q}$, is zero or one. We can apply theorem 2, and by the previous discussion,

$$C(\mathbb{Q}) = \left\{ \left(\frac{4}{121}, \pm\frac{2^5}{11^5} \right), \infty \right\}.$$

We also know that $r = 1$ in this case by corollary 4. We could also conclude this in an other way: Using Magma we see that the torsion subgroup is trivial, which is impossible when $r = 0$ and $\#C(\mathbb{Q}) > 1$.

2.5 Examples on improving lower rank bounds in Magma

We now present two examples of excessive curves, for which we can improve Magma's lower bounds for the rank. In both examples, we can determine the rank of the curve, although Magma gives inconclusive information.

Again, it is desirable to have a small number of residue discs, and in particular, we would like only one residue disc. This time, we will consider $p = 5$ and the curve

$$C : y^2 = 8x^6 - 314x^5 + 3250x^4 - 10000x^3 + 64x = x(2(x-25)(4x-25)(x^3 - 8x^2) + 64).$$

The reduction of C modulo 5 is

$$\overline{C} : y^2 = x(3x^5 + x^4 - 1)/\mathbb{F}_5$$

We easily see that C has good reduction at $p = 5$ and that $\overline{C}(\mathbb{F}_5) = \{(0, 0)\}$. We can find at least five points on this curve,

$$\left\{(0, 0), \left(\frac{25}{4}, \pm 20\right), (25, \pm 40)\right\} \subset C(\mathbb{Q}),$$

so C is excessive. Magma gives us that the rank r of the Jacobian of C satisfies $0 \leq r \leq 2$. Hence, we conclude that $r = 2$.

Note that we do not find the set $C(\mathbb{Q})$ here because Chabauty's condition $r < g$ is violated. It might be possible to compute $C(\mathbb{Q})$ using Quadratic Chabauty.

The following example is conditional, i.e., for the rank computations in Magma we need to assume the Generalized Riemann Hypothesis. We can do the same for the following curve

$$C : y^2 = x^5 - 12(121x - 1)(121x - 4)$$

looking at the good prime $p = 11$. This curve has at least five rational points, so it is excessive. Magma gives us that the rank of its Jacobian over $\mathbb{Q}$ is between zero and two, thus, it is two.

Remark. We see that a curve $C/\mathbb{Q}$ with many rational points (at least $2g-2$) might be potentially sharp or excessive. There is an algorithm to check that. We need to determine all prime numbers p for which C can be potentially sharp or excessive at p. We use the Hasse-Weil bounds and the number of known rational points to give an upper bound for primes p, so we need to check finitely many of them. Therefore, if we find that the curve is potentially sharp, or excessive, we obtain a lower bound for the rank, $r \geq g - 1$, or $r \geq g$, respectively.

Note that here we only considered primes of good reduction. There are results similar to Coleman's bound when we consider primes of bad reduction, and these can be found in [LT02] and improved, with a bound in Stoll's style, in [KZB13]. It would be interesting to investigate the case of bad reduction in the future. In this case, we might be able to construct infinite families of examples with sharp bounds. We could then allow multiple Weierstrass points in the same residue discs, which makes computations of ranks of curves easier and hope that we can determine the ranks of Jacobians for an infinite number of curves.

3 Examples of sharp curves of higher genus

We present a few sharp curves of genus $g > 2$. There is a way to construct potentially sharp curves, which works for any genus g and the construction is contained in § 3.3, including examples sharp curves of genus $g = 4$ and $g = 5$, one of each. In some cases, there is an easier way to find examples of sharp curves, and it is presented in the following subsection.

3.1 Concrete examples of sharp curves of genus three, four and five

Let g be a positive integer. In the case where $2g+1$ or $2g+3$ is a prime number, we can construct potentially sharp curves examples in the following ways.

If $2g+1 = p$, where p is some prime number, then $x^{2g+1} - x \equiv 0 \pmod{p}$ for all $x \in \mathbb{F}_p$. If c is any quadratic nonresidue modulo p, then for the curve

$$\overline{C} : y^2 = x^{2g+1} - x + c/\mathbb{F}_p$$

we have $\overline{C}(\mathbb{F}_p) = \{\infty\}$. So, all possible rational points on the curve C reduce modulo p to ∞, thus are not integral and have denominators divisible by p. Let $a_1, \ldots, a_{g-1}$ be integers not divisible by p, with distinct absolute values. Let $b \in \mathbb{Z}$ be any inverse of $(a_1 \ldots a_{g-1})^2$ modulo p. The following curve is potentially sharp

$$C : y^2 = x^{2g+1} + b(a_1^2 - p^2x) \ldots (a_{g-1}^2 - p^2x)(c - x).$$

If $2g + 3 = p > 3$ is prime, then we can use the property that there are two consecutive quadratic nonresidues modulo p. If $p \equiv 1 \pmod 4$, then between 2 and $p-2$ there are $\frac{p-1}{2}$ quadratic nonresidues implying that two of them must be consecutive. If $p \equiv 3 \pmod 4$, -1 and -4 are quadratic nonresidues, so if -2 or -3 is a quadratic nonresidue, we have the conclusion. If not, then 2 and 3 are consecutive quadratic nonresidues. Denote by c and $c+1$ two consecutive quadratic nonresidues modulo p. Then the curve

$$\overline{C} : y^2 = x^{2g+2} + c/\mathbb{F}_p$$

has two $\mathbb{F}_p$-points, both at infinity because for $x \in \mathbb{F}_p$

$$x^{2g+2} + c \equiv \{c, c+1\} \pmod{p}.$$

We construct examples from this curve. Let $a_1, \ldots, a_{g-1}$ be distinct integers not divisible by p. Let $b \in \mathbb{Z}$ be any inverse of $a_1 \ldots a_{g-1}$ modulo p. The following curve is potentially sharp

$$C' : y^2 = x^{2g+2} + b(a_1 - px) \ldots (a_{g-1} - px)c.$$

We summarize the conclusions above into the theorem.

Theorem 8. *Let $g \geq 2$ be a positive integer such that $2g+1$ or $2g+3$ is a prime number. Define C and C' as above in each case. If r, the rank of the Jacobian of C over $\mathbb{Q}$, satisfies $r < g$, then $r = g-1$, and*

$$C(\mathbb{Q}) = \left\{ \left(\frac{a_1^2}{p^2}, \pm \frac{a_1^{2g+1}}{p^{2g+1}} \right), \ldots, \left(\frac{a_{g-1}^2}{p^2}, \pm \frac{a_{g-1}^{2g+1}}{p^{2g+1}} \right), \infty \right\}.$$

If r', the rank of the Jacobian of C' over $\mathbb{Q}$, satisfies $r' < g$, then $r' = g-1$, and

$$C'(\mathbb{Q}) = \left\{ \left(\frac{a_1}{p}, \pm \frac{a_1^{g+1}}{p^{g+1}} \right), \ldots, \left(\frac{a_{g-1}}{p}, \pm \frac{a_{g-1}^{g+1}}{p^{g+1}} \right), \infty_{\pm} \right\}.$$

Proof. Follows from the above and corollary 4. □

We give one example of a sharp curve in each genus $g \in \{3,4,5\}$. For these curves we are able to check the rank condition $r < g$. However, we need to assume the Generalized Riemann Hypothesis for the rank computations in Magma. The curves are

$$C_3 : y^2 = x^7 - (49x-1)(49x-36)(x+1), \;\; r(J(C_3)(\mathbb{Q})) = 2,$$
$$C_3(\mathbb{Q}) = \left\{ \left(\frac{1}{49}, \pm \frac{1}{7^7} \right), \left(\frac{36}{49}, \pm \frac{6^7}{7^7} \right), \infty \right\};$$
$$C_4 : y^2 = x^{10} - (11x-3)(11x-4)(11x-6), \;\; r(J(C_4)(\mathbb{Q})) = 3,$$
$$C_4(\mathbb{Q}) = \left\{ \left(\frac{3}{11}, \pm \frac{3^5}{11^5} \right), \left(\frac{4}{11}, \pm \frac{4^5}{11^5} \right), \left(\frac{6}{11}, \pm \frac{6^5}{11^5} \right), \infty_{\pm} \right\};$$
$$C_5 : y^2 = x^{12} - (13x-1)(13x-2)(13x-3)(13x-12), \;\; r(J(C_5)(\mathbb{Q})) = 4,$$
$$C_5(\mathbb{Q}) = \left\{ \left(\frac{1}{13}, \pm \frac{1}{13^6} \right), \left(\frac{2}{13}, \pm \frac{2^6}{13^6} \right), \left(\frac{3}{13}, \pm \frac{3^6}{13^6} \right), \left(\frac{12}{13}, \pm \frac{12^6}{13^6} \right), \infty_{\pm} \right\}.$$

3.2 Bertrand's Postulate for primes modulo 8

For our construction, we will need a stronger version of Bertrand's Postulate. We formulate one version first, and then we cover smaller cases.

Proposition 9. *Let $n \geq 15$ be a positive integer. In the interval $[n, 2n)$ there is a prime number p such that $p \equiv 5 \pmod 8$.*

Proof. Let $\mathbb{P}$ denote the set of prime numbers in $\mathbb{Z}$. For any coprime integers k and l, we define the function

$$\theta(x; k, l) = \sum_{p \in \mathbb{P},\ p \leq x,\ p \equiv l (\mathrm{mod}\ k)} \log(p).$$

Theorem 1, for $k \leq 13$, from [RR96], states that

$$\max_{1 \leq y \leq x} \left| \theta(y; k, l) - \frac{y}{\varphi(k)} \right| \leq \varepsilon \frac{x}{\varphi(k)},$$

where one can take $\varepsilon = 0.00456$ for $x \geq 10^{10}$. It implies that when $y = x$

$$\left| \theta(x; 8, 5) - \frac{x}{4} \right| \leq 0.00456 \frac{x}{4} \leq 0.005 \frac{x}{4} \implies 0.995 \frac{x}{4} \leq \theta(x; 8, 5) \leq 1.005 \frac{x}{4}$$

for $x \geq 10^{10}$. If $x \geq 10^{10}$, then also

$$\theta(x; 8, 5) \leq 1.005 \frac{x}{4} < 0.995 \frac{2x}{4} \leq \theta(2x; 8, 5)$$

giving that $\theta(2x; 8, 5) > \theta(x; 8, 5)$ for $x \geq 10^{10}$. It follows that there is a prime congruent to 5 modulo 8 between x and $2x$. We need to prove the statement for the remaining interval $[15, 10^{10}]$. We can easily find a list of primes congruent to 5 modulo 8 such that the next one is larger than half of the previous one (e.g., we can use Magma for it), which completes the proof. For instance, we can take the list to be

$$10000000061, 5000000141, 2500000117, 1250000077, 625000069, 312500077, 156250093,$$

$$78125141, 39062581, 19531381, 9765757, 4882957, 2441573, 1220797, 610429, 305237,$$

$$152629, 76333, 38189, 19141, 9613, 4813, 2437, 1229, 653, 349, 181, 101, 53, 29.$$

□

Proposition 10. *Let $n \geq 2$ be a positive integer. Then in the interval $[n, 2n)$ there is a prime number p such that $p \equiv 3 \pmod 8$ or $p \equiv 5 \pmod 8$.*

Proof. By the previous proposition, we only need to check small cases, but the statement is trivially true since 3, 5, 11, 19 are primes that fill in the missing gaps. □

As a corollary, in each interval $[n, 2n)$, where $n > 1$ is a positive integer, there is a prime p such that 2 is not a quadratic residue modulo p, which is the property we will use in our construction of curves in the following subsection.

3.3 Potentially sharp curves in genus $g \geq 2$

Let $g \geq 2$ be a positive integer. We will construct potentially sharp hyperelliptic curves $C : y^2 = f(x)$ of genus g, where f is a monic polynomial. For simplicity, we present the construction and ideas in a simpler way. We add a comment on how we can slightly generalize it using the same ideas after theorem 12 and use these generalized ideas to construct concrete examples.

By our version of Bertrand's postulate, proposition 10, there is a prime number p, congruent to 3 or 5 modulo 8, which is contained in the interval $(2g+2, 4g+4)$. Define the polynomial

$$Q(x) = x^{2g+2} - x^{\frac{p-1}{2}} + x^{2g+2-\frac{p-1}{2}} + 1.$$

Then we have the following congruence modulo p

$$Q(x) \equiv \begin{cases} 2x^{2g+2} \pmod{p}, \text{if } \left(\frac{x}{p}\right) = 1, \\ 2 \pmod{p}, \text{if } \left(\frac{x}{p}\right) = -1, \\ 1 \pmod{p}, \text{if } p \mid x. \end{cases}$$

Since p is chosen so that 2 is quadratic nonresidue modulo p, it follows that

$$\overline{C}(\mathbb{F}_p) = \{(0, \pm 1), \infty_{\pm}\},$$

if $\overline{C}$ is the hyperelliptic curve over $\mathbb{F}_p$, defined by $y^2 = Q(x)$.

For each $s \leq g$, $s \in \mathbb{N}$, we will construct curves $C_s : y^2 = H_s$, whose reduction modulo p is $\overline{C}$ and which will have at least $4+2s$ rational points. Four rational points on C_s will be from the set $\{(0, \pm 1), \infty_{\pm}\}$, and we need to add $2s$ points, i.e. s values of x for which $H_s(x)$ is a square of a rational number. We will construct H_s such that new rational points on C_s are integral, so that all x-coordinates will be integers divisible by p. We note that then C_{g-1} is a potentially sharp curve and C_g excessive.

Let $a_1, \ldots, a_s \in \mathbb{Z}$ be distinct and non-zero. We will construct the polynomial H_s such that $H_s(pa_1)$, $H_s(pa_2)$, ..., $H_s(pa_s)$ are squares of integer numbers. The strategy is as follows. All monomials x^k with $k > s$ will be replaced by

$$t_s(x^k) := x^{k-s}(x - pa_1)(x - pa_2)\ldots(x - pa_s).$$

We extend this transformation linearly so that we can compute $t_s(P) \in \mathbb{Z}[x]$ for all polynomials $P \in \mathbb{Z}[x]$ which have only monomials in x of degree greater than s. This transformation has two important properties, namely for all such $P \in \mathbb{Z}[x]$

$$t_s(P) \equiv P \pmod{p},$$

$$t_s(P)(0) = t_s(P)(pa_1) = \ldots = t_s(P)(pa_s) = 0.$$

We can apply this transformation to the higher degree part of $Q(x)$, e.g. to the polynomial $x^{2g+2} - x^{\frac{p-1}{2}}$ (note that $\frac{p-1}{2} > g \geq s$). We need to deal with the remaining part $1 + x^l$, where $l := 2g + 2 - \frac{p-1}{2}$. If $l > s$, then we can apply t_s to x^l and define a polynomial

$$Z_s(x) := t_s(x^{2g+2} - x^{\frac{p-1}{2}} + x^l) + 1.$$

If $s \geq l$, the polynomial $1 + x^l$ will be transformed into a part of a square of some polynomial. In this way, we can assure that $H_s(pa_i)$ is a square for $i = 1, \ldots, s$. Denote $m \in \mathbb{N}$ the number for which $ml \leq s < (m+1)l$. We use the following lemma.

Lemma 11. *There exist integers c_1, c_2, ..., c_m such that*

$$(1 + c_1 x^l + c_2 x^{2l} + \ldots + c_m x^{ml})^2 \equiv 1 + x^l \pmod{p, x^s},$$

meaning that these two polynomials agree modulo p up to degree s.

Proof. We prove this lemma constructively. We can start by taking $c_1 = \frac{p+1}{2}$ (or any other number congruent modulo p to it). Then, looking at coefficients with x^{jl}, where $j \in \{2, \ldots, m\}$ we have

$$2c_j + S_j \equiv 0 \pmod{p},$$

where S_j is some polynomial in the previous coefficients c_1, ..., c_{j-1}. Since p is odd, 2 is invertible and we can determine c_j modulo p. □

If c_j are the coefficients from the previous lemma, then

$$(1 + c_1 x^l + c_2 x^{2l} + \ldots + c_m x^{ml})^2 = G_s(x) + L_s(x),$$

where $\deg(L_s) \leq s$ and $L_s(x) \equiv 1 + x^l \pmod{p}$, and all monomials in x in G_s have degree at least $s+1$. Note $\deg(G_s) = 2ml \leq 2s < 2g+2$. Define the polynomial Z_s as

$$Z_s(x) = t_s(x^{2g+2} - x^{\frac{p-1}{2}} - G_s(x)) + G_s(x) + L_s(x).$$

In both cases ($l > s$ and $s \geq l$) for all $i = 1, \ldots, s$, we have

$$Z_s(pa_i) = G_s(pa_i) + L_s(pa_i) = (1 + c_1 p^l a_i^l + c_2 p^{2l} a_i^{2l} + \ldots + c_m p^{ml} a_i^{ml})^2 =: b_i^2,$$

where, if $l > s$, $c_1 = \ldots = c_m = 0$, i.e. $b_1 = \ldots = b_s = 1$, $Z_s(0) = 1$, and

$$Z_s(x) \equiv x^{2g+2} - x^{\frac{p-1}{2}} + x^l + 1 = Q(x) \pmod{p}.$$

We can change Z_s by any polynomial $px(x - pa_1)\ldots(x - pa_s)R(x)$, where $R \in \mathbb{Z}[x]$ has degree at most $2g - s$, and the new curve will still have all known rational points and the same reduction modulo p. So, for any choice as above, define

$$C_s : y^2 = H_s(x), \;\; H_s(x) := Z_s(x) + px(x - pa_1)\ldots(x - pa_s)R(x).$$

Note that we can take $b_i \equiv 1 \pmod{p}$, so $b_i \neq 0$, and we indeed have at least $4 + 2s$ rational points on C_s:

$$\{\infty_\pm, (0, \pm 1), (pa_1, \pm b_1), \ldots, (pa_s, \pm b_s)\} \subset C_s(\mathbb{Q}).$$

Therefore, we constructed many examples of potentially sharp curves C_{g-1} and curves C_g of large rank. Let r_s be the rank of the Mordell-Weil group of the Jacobian of C_s over $\mathbb{Q}$. We summarize this in the following theorem.

Theorem 12. *(1) Let $s = g-1$, i.e., let C_{g-1} be a curve defined as above. If $r_{g-1} < g$, then $r_{g-1} = g-1$, and*

$$C_{g-1}(\mathbb{Q}) = \{\infty_{\pm}, (0, \pm 1), (pa_1, \pm b_1), \ldots, (pa_{g-1}, \pm b_{g-1})\}.$$

(2) Let $s = g$, i.e., let C_g be a curve defined as above. Then $r_g \geq g$.

Proof. (1) By construction, C_{g-1} is potentially sharp. If the rank condition is satisfied, then C_{g-1} is sharp, hence has exactly $2g+2$ points and rank $r_{g-1} = g-1$.
(2) The curve C_g is constructed to be excessive, so $r_g \geq g$. □

Comment. In the spirit of the ideas in the construction, we can change the curves in the following ways.
(1) The transformation t_s can be slightly changed as $(k > e_1 + \cdots + e_s)$

$$t_{e_1,\ldots,e_s}(x^k) = x^{k-e_1-\cdots-e_s}(x-pa_1)^{e_1}(x-pa_2)^{e_2}\ldots(x-pa_s)^{e_s}.$$

(2) The numbers $a_1, \ldots, a_s$ do not have to be integers, we can allow them to be rational numbers, such that $a_i = \frac{b_i}{c_i}$, $\mathrm{GCD}(b_i, c_i) = 1$, $p \mid b_i$ for all $i = 1, \ldots, s$, but we need to be careful to make sure that the curve still has two points at infinity. Note that the resulting polynomial, after a linear change of variables, might not be monic anymore.
(3) We can change anything modulo p, so that the reduction curve stays the same, as long as we do not change the number of known rational points. For example, the constant term of the polynomial can be any square of an integer congruent to 1 modulo p, or we can change the polynomials constructed in lemma 11, or increase their degree until it is not greater than g, and similar constructions.

Based on the above construction, we have searched for examples of sharp curves using Magma. We were unable to find sharp examples of genus two or three. For these genera, the generic rank of the subgroup generated differences of the rational points on the curve appears to be at least g. We give one example of a sharp curve of genus four, and one example of a sharp curve of genus five. For both examples, we assume the Generalized Riemann Hypothesis to compute the rank. We did not check the rank conditions of curves of genus at least six, since this is a computationally extremely difficult task.

We start with a curve of genus four. We choose the prime $p = 11$. Then the reduction modulo 11 is the curve $\overline{C} : y^2 = x^{10} + 1$. Since there are no small powers of x, we only need to add more rational points using some convenient t transformation. We consider the curve

$$C : y^2 = x^4(x-11)^2(x-22)^2(x-33)^2 + 1.$$

This curve has the property that the element $[\infty_- - \infty_+]$ of the Jacobian has finite order 5, increasing the chances chances to obtain smaller rank. Indeed, it is verified in Magma that this curve has rank 3, so it is a sharp curve of genus four, and

$$C(\mathbb{Q}) = \{\infty_\pm, (0, \pm 1), (11, \pm 1), (22, \pm 1), (33, \pm 1)\}.$$

We use a similar strategy to construct a sharp curve of genus five. We choose $p = 13$, and start with the reduction curve $\overline{C} : y^2 = x^{12} + 1$. Then we consider the curve

$$C' : y^2 = x^4 \left(x^2 - \frac{13^2}{3^2}\right)^2 \left(x^2 - \frac{13^2}{4^2}\right)^2 + 1,$$

or, after the linear change of variables

$$C : y^2 = x^4(9x^2 - 169)^2(16x^2 - 169)^2 + 144^2.$$

This curve is potentially sharp, as $\#\overline{C}(\mathbb{F}_{13}) = 4$, and $\#C(\mathbb{Q}) \geq 12$. Hence, the rank of its Jacobian satisfies $r \geq 4$.
The group of automorphisms of C contains the group $(\mathbb{Z}/2\mathbb{Z})^2$, so by [Pau08, 3.1.1., Theorem 5], C has two quotients of degree two, C_1, and C_2, such that $J(C)$ is isogenous to the product $J(C_1) \times J(C_2)$. We conclude that the rank of $J(C)$ is equal to the sum of ranks of $J(C_1)$ and $J(C_2)$. Using Magma, we compute that C_1 and C_2 given by the equations

$C_1 : y^2 + (x^2 + x)y = 5184x^6 + 37944x^5 - 802992x^4 - 3580910x^3 + 35285157x^2 + 32655315x + 7268209,$

$C_2 : y^2 = -20736x^7 - 55584x^6 + 4461023x^5 + 5168390x^4 - 294280801x^3 - 78257128x^2 + 4786378304x + 8098228736.$

Furthermore, for both curves C_1 and C_2, Magma gives the lower rank bound 0, and the upper bound 2. We conclude that both $J(C_1)$ and $J(C_2)$ have rank 2, because the sum of their ranks is at least 4. So the curve C has rank 4, it is sharp, and

$$C(\mathbb{Q}) = \left\{\infty_\pm, (0, \pm 144), \left(\pm\frac{13}{3}, \pm 12\right), \left(\pm\frac{13}{4}, \pm 12\right)\right\}.$$

We note that it might be possible to use the method of Chabuaty and Coleman to find the rational points on C_2, and to use that information to find $C(\mathbb{Q})$. However, the curve C_2 is not sharp, so it would be more involved to compute the set $C_2(\mathbb{Q})$.

References

[BBM16] Jennifer S. Balakrishnan, Amnon Besser, and J. Steffen Müller. Quadratic chabauty: p-adic heights and integral points on hyperelliptic curves. *Journal für die reine und angewandte Mathematik*, 2016(720):51 – 79, 01 Nov. 2016. 1.1

[BBM17] Jennifer Balakrishnan, Amnon Besser, and J. Steffen Müller. Computing integral points on hyperelliptic curves using quadratic Chabauty. *Mathematics of Computation*, 86:1403–1434, 2017. 1.1

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3–4):235–265, 1997. 1

[BS09] Nils Bruin and Michael Stoll. Two-cover descent on hyperelliptic curves. *Mathematics of Computation*, 78(268):2347–2370, 2009. 1.3

[BS10] Nils Bruin and Michael Stoll. The Mordell–Weil sieve: proving non-existence of rational points on curves. *LMS Journal of Computation and Mathematics*, 13:272–306, 2010. 1.1

[Cha41] Claude Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941. 1

[Col85a] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 09 1985. 2, 2.1

[Col85b] Robert F. Coleman. Torsion points on curves and p-adic abelian integrals. *Annals of Mathematics*, 121(1):111–168, 1985. 1.1

[Dok04] Tim Dokchitser. Computing special values of motivic L-functions. *Experimental Mathematics*, 13(2):137–149, 2004. 1.2

[Fal83] Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inventiones Mathematicae*, 73(3):349–366, 1983. 1.1

[GG93] Daniel M. Gordon and David J. W. Grant. Computing the Mordell-Weil rank of Jacobians of curves of genus two. *Transactions of the American Mathematical Society*, 337(2):807–824, 1993. 1.2, 2.1

[Gra94] David Grant. A curve for which Coleman's effective Chabauty bound is sharp. *Proceedings of the American Mathematical Society*, 122(1):317–319, 1994. 2.1, 2.2

[HM19] Yoshinosuke Hirakawa and Hideki Matsumura. A unique pair of triangles. *Journal of Number Theory*, 194:297 – 302, 2019. 2.1

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine geometry. An Introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. 1.2

[HZ02] Everett W. Howe and Hui June Zhu. On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field. *Journal of Number Theory*, 92(1):139 – 163, 2002. 2.2, 5

[Kim05] M. Kim. The motivic fundamental group of $\mathbb{P}^1\backslash\{0,1,\infty\}$ and the theorem of Siegel. *Inventiones mathematicae*, 161(3):629–656, 2005. 1.1

[KZB13] Eric Katz and David Zureick-Brown. The Chabauty–Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions. *Compositio Mathematica*, 149(11):1818–1838, 2013. 2.5

[LT02] Dino Lorenzini and Thomas J. Tucker. Thue equations and the method of Chabauty-Coleman. *Invent. Math.*, 148(1):47–77, 2002. 2.5

[Mor22] Louis J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Phil. Soc.*, 21:179–192, 1922. 1.1

[MP12] William McCallum and Bjorn Poonen. The method of Chabauty and Coleman. *Explicit methods in number theory, Panor. Synthèses*, 36:99–117, 2012. 1.1

[Pau08] Jennifer Paulhus. Decomposing Jacobians of curves with extra automorphisms. *Acta Arith.*, 132(3):231–244, 2008. 3.3

[RR96] Olivier Ramaré and Robert Rumely. Primes in arithmetic progressions. *Mathematics of Computation*, 65(213):397–425, 1996. 3.2

[Sch95] Edward F. Schaefer. 2-descent on the Jacobians of hyperelliptic curves. *Journal of Number Theory*, 51(2):219 – 232, 1995. 1.2

[Sch99] Victor Scharaschkin. Local-global problems and the Brauer-Manin obstruction. *ProQuest LLC, Ann Arbor, MI, Thesis (Ph.D.)–University of Michigan*, 1999. 1.1

[Sik15] Samir Siksek. Chabauty and the Mordell-Weil sieve. In *Advances on superelliptic curves and their applications*, volume 41 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, pages 194–224. IOS, Amsterdam, 2015. 1.1

[Sto01] Michael Stoll. Implementing 2-descent for Jacobians of hyperelliptic curves. *Acta Arith*, 98(3):245–277, 2001. 1.2

[Sto06] Michael Stoll. Independence of rational points on twists of a given curve. *Compositio Mathematica*, 142(5), 04 2006. 1.1, 3

[Sto15] Michael Stoll. Descent and covering collections. In *Advances on superelliptic curves and their applications*, volume 41 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, pages 176–193. IOS, Amsterdam, 2015. 1.3

[Tat66] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. pages Exp. No. 306, 415–440, 1966. 1.2

[Wei29] André Weil. L'arithmétique sur les courbes algébriques. *Acta Math.*, 52(1):281–315, 1929. 1.1